Journal of Computing & Biomedical Informatics
ISSN:2710-1606

Volume 09 Issue 01
2025

Research Article
https://doi.org/10.56979/901/2025

Fine Decision Tree Outperforms in Early Intrusion Detection: A Supervised Learning Comparison on NSL-KDD and NID

Muhammad Zubair Khan[1], Naveed Mukhtar[2], Aaliya Ali[3], Tahira Ali[4], Waqar Hussain[5], Muhammad Farrukh Khan[6], Zahid Iqbal[7], Gullelala Jadoon[8], and Shahan Yamin Siddiqui[9*]

[1]Department of Computer Science, Green International University, Lahore, Pakistan.
[2]Faculty of Computer Science & Information Technology, Superior University, Lahore, Pakistan.
[3]Department of Computer Science, Pakistan Navy Engineering College, NUST, Pakistan.
[4]Computer Science and Information Technology Department, NED University of Engineering and Technology, Pakistan.
[5]Department of Artificial Intelligence, University of Kotli Azad Kashmir, Pakistan.
[6]Department Artificial intelligence, NASTP institute of Information Technology, Lahore, Pakistan.
[7]School of Computer Science, Minhaj University Lahore, Pakistan.
[8]Department of Information Technology, University of Haripur, Pakistan.
[9]Department Computer Science, NASTP institute of Information Technology, Lahore, Pakistan.
[*]Corresponding Author: Shahan Yamin Siddiqui. Email: drshahan@niit.edu.pk

Received: April 06, 2025 **Accepted:** May 26, 2025

Abstract: The intrusion detection system plays a major role towards network security, to prevent network threats. An intrusion detection system is used to keep track of network or systems activity in a bid to detect any mischievous activity. The dataset containing intrusion attacks is used to detect abnormalities in the network with the help of the machine learning algorithm. Machine learning has three major subcategories, which include supervised, unsupervised, as well as reinforcement learning. The most common and the most important supervised learning classifiers are used in machine learning. The most scholar has been looking on the intrusion detection through various machine-learning methods. Nevertheless, it still brings out some weaknesses. In order to identify the most successful supervised machine learning algorithm that could be used in detecting intrusions. This paper used the two feature-based datasets, namely NSL_KDD and NID and the five supervised machine learning algorithms, such as Support Vector Machine, Naive Bayes, Logistics Regression, Decision Tree and Neural Networks. Those algorithms can be used in an intrusion detection system, however, the comparison of the results demonstrates their efficiency. It also recommends the best approach which should be adopted so as to prevent attacks at an early stage in this field. The fine Decision Tree algorithm had an accuracy of 99.4%, which is better in identifying intrusions at the beginning. Their performance is far much better when compared to other algorithms.

Keywords: Intrusion Detection System (IDS); Machine Learning (ML); Support Vector Machine (SVM); Naive Bayes (NB); Logistics Regression (LR); Decision Tree (DT); Neural Networks (NN)

1. Introduction

The technology ecosystem is changing in the most amazing speed. As of the statistic of the Internet usage in the world in 2022, half of the entire world population (4.9 billion people) makes use of internet [1] It is the act of securing a computer network against its possible vulnerabilities and weaknesses in order to protect.

Protection is performed in order to maintain it with terms of accessibility and integrity as well. The network security process is to provide protection of a network against a broad variety of the attacks normally referred to as an incursion as well as the prevention of the attacks to penetrate and propagate within the network [2].

Intrusion is defined as a group of actions, which may be executed to a computer network but the actions infringe established security of the network. In the recent years, we have witnessed numerous cyber-attacks in most companies across the world. In the year 1972, Bob Thomas created a computer program, called the Creeper, which was an experimenter term of the ARPANET research program [3]

The phase between the 1990s and the 2000s experienced an unprecedented boost in the number of people engaging in and accessing the internet whose resulting outcome was a marked increment in the amount of information available on the internet [4]. The situation has led to an outburst of cyber-attackers who gravitate to use the new powers of the internet to steal confidential information of different organizations as well as governments and individuals. Moreover, there was an antivirus software explosion in a bid to respond to the arising security issues.

Malware has evolved throughout the years to change the design of intrusion detection mechanisms as reflected by the current survey on cyber-attacks. There are a number of attacks used by hackers to access sensitive information in the modern world. There are various types and causes of intrusion that should be controlled since, in case of its absence, it has organizational impacts [5]. Intrusion Detection System monitors the network traffic and data produced by the hosts and checks them against security violations. Malicious individuals have employed different fraud tactics of concealing data and hiding their tempered data this has prompted the significance of the identification process of malware whose source of attacks is unknown and that which is disguised.

Intrusion Detection Systems (IDS) are described as the hardware and piece of software used to identify and limit possible interference. Intrusion Detection Systems ensure scanning of hostile operations and break of security and they alert the administrators of the system of unusual movement. Such malicious activities cannot be found by utilizing conventional firewall, since its functionality is limited to the OSI Transport Layer. The illegal entry, hacking, and misuse of the use of the computer networks by the internal and external intrusions are called computer intrusion [6]. The strategy has been formulated as a rule-based, expert program that can detect predetermined intrusions. There are two types of intrusion detection systems (IDS), such as host-based and network-based [7].

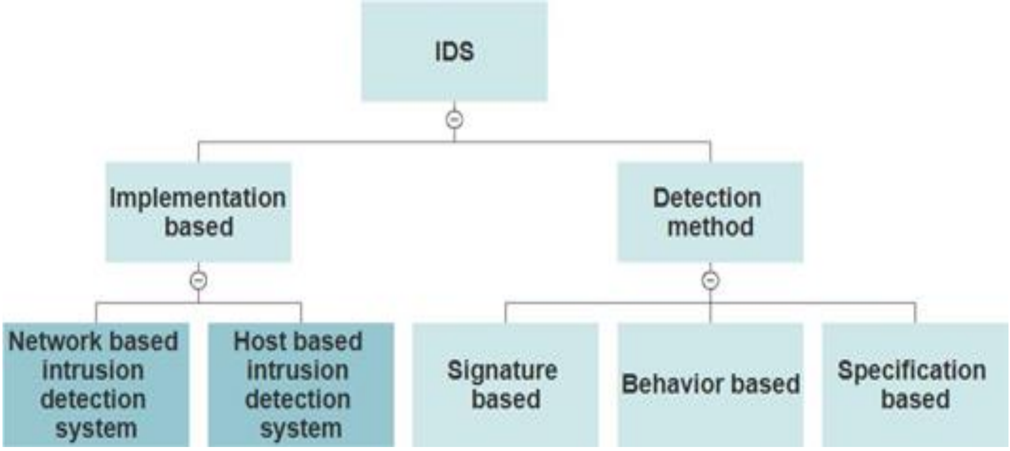


Figure 1. Intrusion Detection System Classification [11]

The information technology has become fast-growing and in result, more network equipment and network services are used. The demand has increased tremendously with the emergence of remote work, virtual meeting, online education, e-commerce and online entertainment. As the new normal is pushing itself, the vulnerability surface is growing by leaps and bounds and therefore the dishonest parties are taking note of the matter because the frequency of cyber-attacks has grown by an enormous margin.

Cisco collated the Future of Secure Remote Work Report through global study poll of 21 markets. Based on the theoretical research of one of the studies conducted by [8], it grew by an astronomical amount to reach 62 percent of people who were forced to join the remote workforce during the pandemic. And to be precise, 85 percent of all the respondents all over the world, have made a statement regarding their argument that cybersecurity has now become extremely vital or it has gained more importance than it already was prior to in the pandemic.

A majority of the survey participants, 61 per cent, stated that their threats or warnings of cyber-attack had grown by 25 per cent or more since the onset of the COVID-19 pandemic. The results of the distribution of these threats or warnings in the multiple regions i.e. Global, ADPJ, AMER and Europe are discussed. Markedly, 8 out of every 100 businesses in the world are ignorant of their current status of cyber threat/alerts. It implies that they have not experienced any form of cyber-attacks which is out of tune with the current scenario of cyber-attacks or that they are unable to pick them. Ordinarily, to the majority of organizations, the latter is a deplorable situation that should be considered keenly.

Artificial intelligence is the aspect of programming the computer to imitate human intelligence and make the devices perform similar intelligence and behaviors that human beings can achieve [9]. Due to the blistering pace at which interest in the area of AI has grown, vendors have sought to push to the fore the means of their products and services integrating well with this technology. In many occasions, the term AI may only refer to one of the components of the technology, e.g. machine learning [10]. The machine learning algorithms employ past data as the input in order to predict output values. Supervised learning in Machine Learning (ML) introduces labelled data sets wherein the outcome of applying the expected input can be ascertained whereas unsupervised learning uses unlabeled data sets to help ascertain the desired outcome based on initially unknown results.

Machine Learning Model will assist in training the system in predicting the intrusion in the network even before it has the capacity to cause harm or even cut the network traffic which will save on resources employed by the system in time spent in processing it. The present paper shows two featured based intrusion sets, which can be availed online possessing multiple features and outputs as Normal and Anomaly in order to detect the incidence of intrusions in accordance with particular standards using continuous things as well as claiming adequate accuracy to be obtained. Comparison will be conducted between these five approaches in order to enhance intrusion analysis.

2. Related Work

The phase involves a detailed understanding of the existing situation of Intrusion Detection Systems (IDS) software and research of machine learning problems. Many research projects and failures were completed in several years to develop an intrusion detection system based on the methodology of machine learning.

The feature description through cluster center and nearest neighbor [10] was proposed. The procedure was calculated on the following two measurements. Last of all, information is compared to the nearest cluster member. This is regarded to be the closest neighbor. Such a new distance is one dimensional with respect to area. This is necessary to enable an intrusion detection because it can defining each of the data samples with a K-NN appropriately. Also, it can be used in high effectiveness when processing in the stages of training and testing categorization development.

To detect the said incursions, Narayan and [11] combined C4.5 algorithm, Naive Bayes algorithm. Then, C4.5 algorithm will be applied in modeling to develop a model that will be used in detecting the inappropriate use. This follows the other initial step which involves further partitioning of the data to be used in training into more tiny parts. These subsets, being of different varieties, feed into multiple models of Naive Bayes algorithm (one-class). Mixed classifier is considered as a modifier to enhance the entire working of the IDS as well to decrease its training time. On the other hand, it turned out that the most inaccurate procedure was that of the Random Tree which was also time consuming. The C4.5 algorithm, Naive Bayes and Decision Tree algorithm showed maximum complication even though the results were accurately projected.

According to [12], the use of classifier on the IDSs has improved through its integration with the supervised manner of learning along with the proposed fuzziness-based semi-supervised learning method. This was then proceeded by the uncertain quantity test that was administered on the samples that had been not accurately identified. Such results are based on the data analysis of the data. Along with that, the results of this study confirm that the samples of the class with the fuzziness level closest to the point in the middle of the scale are more likely to be misclassified by the IDS.

Machine learning can enable software apps to be better at detecting new attacks and preventing unlawful entry without the necessity of an express design [13]. Such algorithms will automatically identify and categorize possible risks to the security of a system. It is enabled thanks to the algorithm acquiring knowledge out of all past experience and re-working on this knowledge. It forms a measurement identification model that can be used to classify the traffics on the network and these algorithms require access to the applicable input data.

[14] Estimated the accuracy of IDS system, in the basis of J48, Random Forest, Decision Tree, and Logistic Model. The three data splits were applied in determining the most accurate algorithm to apply in generating further predictions. Compare the accuracy, execution time, f- measure, roc curve and precision. Artificial neural networks can be used to handle patterns- both linear and irregular ones. The recovered model is calculated by making use of the qualities of the intrusion. A method of detection using ANN was presented [15]. KDD Cup 99 incursion classification was done using Neural Networks that are learned using backpropagation and feedforward. This group of knowledge encompasses details on the operation of networks. This approach was found to have the precision of 94.93%.

As indicated by [16], intrusion detection was outperformed by the support vector computers. The structure of the Support Vector Machine (SVM) possesses a lot of computational benefits, some of which are being of particular orientation at a constrained sample, being indifferent of the complexity of algorithm as well as depending on an irrelevant dimension of a sample. Besides, among the support machines (SVMs) advantages, multiple advantages are random forests, decision trees, multilevel perceptrons, etc. This machine-learning model was tested and trained in the researcher using NSL-KDD. Filter selections deleted undesired characteristics in the dataset. The current detection model makes use of a support vector machine classifier because it proves to be a formidable and sound approach in the training data. Therefore, the feature selection method reduces the dimensionality of the datasets and the complexity of computations. The suggested plan has an accuracy of 97.97%, 98.79%, 97.17% and 99.1 percentage.

A medical cyber-physical-specific intrusion detection system (IDS) was developed by [17]. The NSLKDD set helped in training and evaluating the classifier and thus it was simple to port to a typical network structure. We applied a binary classification with 2-layer deep Multilayer Perceptron (MLP) neural network. The transformation of a five-class scenario to two-class predicament is fascinating. The neural network labels the information as belonging to the attack, or otherwise. The NSLKDD dataset integrated 38 subtypes and there are only 16 of them within these attacks. It explains that they use the "evolved 2-class" technique because this method requires less time in its training and can more accurately label instances as compared to a majority of classifiers that use 5 classes. On the contrary, the 5-class classifier will take 264.19 sec to train and the detection rate becomes 98.0 %.

3. Proposed Methodology

In this section the two datasets of this experiment have been described, the proposed methodology including the steps of methodology along with the process of feature selection and the classification techniques of supervised machine learning and how they work.

3.1. Network Security Datasets Details

This study uses the two different featured-based intrusion datasets. Such information is retrieved through internet sources and the results are brought under two categories Normal and Anomaly to reveal the intrusion.

3.1.1. Network Dataset NSL_KDD Description

Over the last three decades, intrusion detection systems have evolved to a great extent. NSL KDD 99 cup is one of the most common intrusion detection datasets. Nonetheless, there are 42 attributes only (41 inputs and 1 output variable) of the NSL-KDD dataset. The above characteristics may be categorized to be a typical or an attack on the NSL-KDD dataset. The training set of the NSL-KDD is a set of 125,973 cases. The authors assume that NSL-KDD dataset is of the right size, which makes it programmatically plausible to apply the whole dataset and not use random sampling. In addition, this method provides consistent and similar results in different research initiatives.

3.1.2. Network Dataset NID Description

The second data is Network Intrusion Detection (NID) which is an instrumental set of data gathered out of Kaggle source and consisted of a number of simulated network intrusions. In the class variable, there are two separate groups, i.e. Normal and Anomaly. NID dataset includes 42 characteristics, 41 characteristics are inputs, and one characteristic is outputs. These attributes can be classified as regular or attack of NID dataset. There are a total of 25192 records on the data set.

3.2. Proposed IDS Architecture with ML Approaches

Three main layers going to comprise the conceptual model namely; data acquisition layer, preprocessing layer and application layer. It is also based on two layer in application. The latter is the first one training model and second is the evaluation layer and it can be viewed in the below mentioned figure 2.

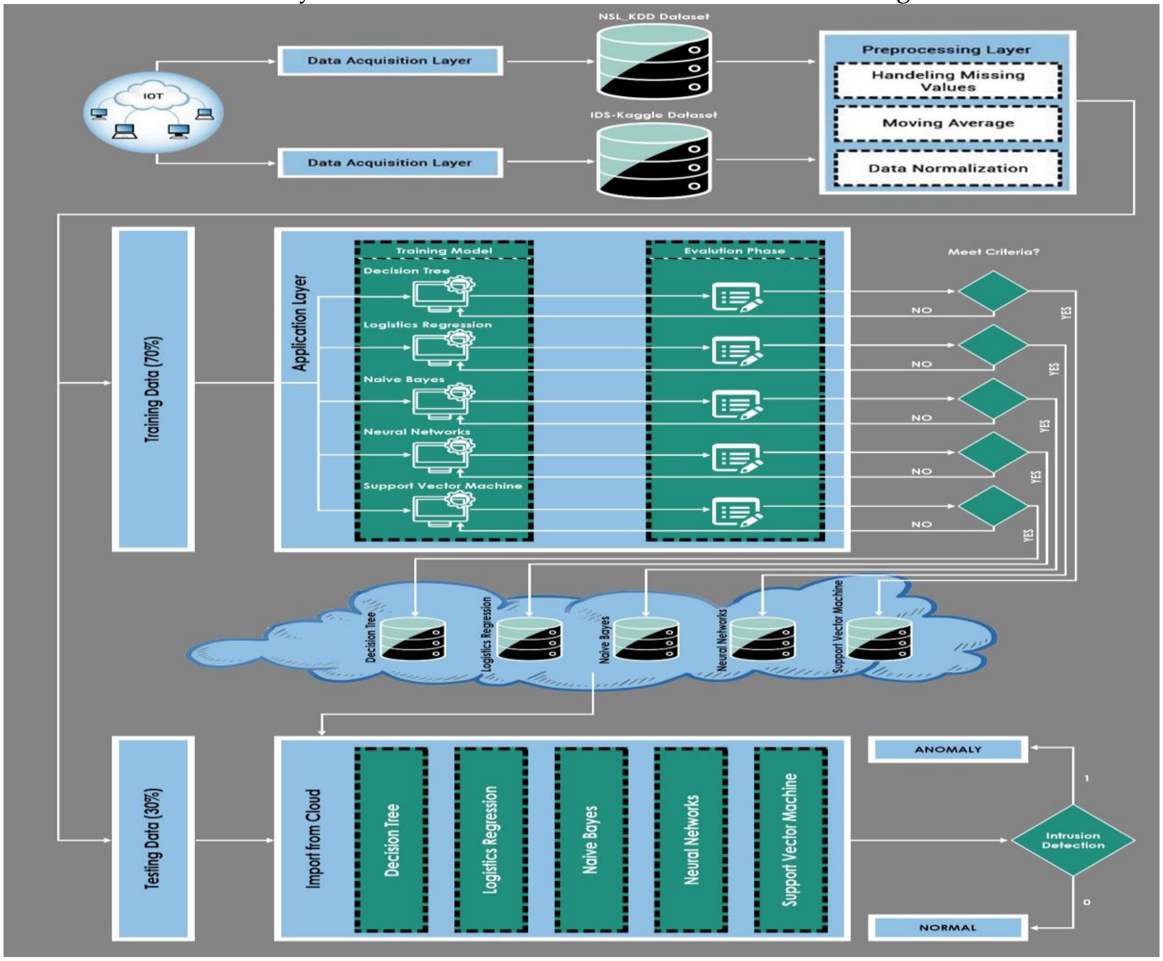


Figure 2. Proposed IDS Model on NSL and IDS Datasets

3.2.1. Dataset Gathering

Initially the IoT devices would collect data of different heterogeneous sensors which is portrayed by IoT in the figure. Once the data is gathered with the aid of such devices then it is referred to as data acquisition layer. Two sources of data online, primarily, Kaggle and Candian repository are utilized in acquiring data in intrusion datasets of proposed systems. These platform collects the data that can be located in sensory section of model. At that stage, the data has been obtained and has been stored in the database as raw because data created by a device can never be tidy and orderly; rather it is always littered by some sort of noise, irregulity, and distortion on it. Data will be collected in the sensors and then raw material will be saved.

3.2.2. Data Normalization and Preprocessing

Another process that cannot be ignored before the model training is implemented is the data pre-processing. We can find it efficient to apply preprocessing techniques such as outlier filters, peak missing value imputation, eliminating duplicates, put categorical variables at numeric format as integer, and tend to data normalization techniques. NSL_KDD and NID datasets were utilized to train the model and subsequently test the model in the study. The abnormalisation operates by marking the normal 0 and an unusual 1 as in the screenshot attached below. The shown graph illustrates a normal and anomaly output classification figures. The normal parameters have blue color whereas parameters of anomaly are orange.

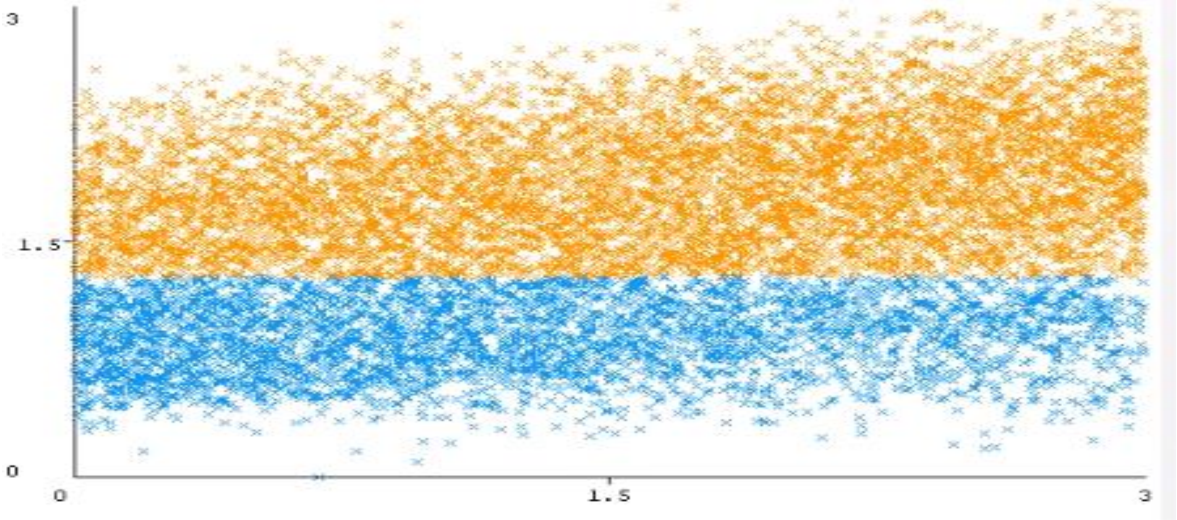


Figure 3. Preprocessing Visualization of Output Feature Values

3.2.3. Prediction Layer

The application layer which constitutes two other sub layers is the third layer in the proposed model. After preprocessing, the data will be divided into 2 groups i.e. training and test set; 70 percent of the data should be used to train propose and 30 percent to test propose as shown in Figure 2.

3.2.3.1. Model Training Phase

The model proposed in it applies these five different supervised machine-learning procedures to train and test. The 70 percentage NSL_KDD and NID records were have been tested with the 5 classifications (i.e., Logistic Regression, Naive Bayes, Support Vector Machine, Neural Network, and Decision Tree). Once the model has undergone training, check the level of the accuracy and how often the model makes an error. The test data labels may be predicted through these models.

3.2.3.2. Performance Phase

Upon training the model, a comparison about predicted labels and actual labels is made. The calculations are performed so as to quantify the precision, the proportion of true positives, and the proportion of false positive. These are those parameters which can be used to compare the performance of the work of the models. When the trained model is able to overcome the example presented in learning criteria then the model is stored to the database and otherwise the retraining of the model occurs when that has been trained enough and load to the validation phase in order to re-test the model using the remaining 30 percent data. The 30 percent data goes through the processing and then it is handed over to the application and its part here where the import-trained model is cloud-mapped with the phase data of validation. When the system detects the target with which it can detect infiltration, then the system ought to be instructed to stop the attack and in circumstances whereby it cannot do this then the element ought to be removed.

4. Results and Simulation

The results of the proposed Model were obtained with the help of MATLAB based on supervised computer learning methods. It has been using two features-based datasets. This study involves support machine vectors and neural networks, decision trees, naive Bayes and logistic regression. The proposed model is training and validation. At training stage, 70 per cent of data will be in use whereas 30 per cent will be used in the test mode. The model to be proposed applies the Binary class classification.

4.1. Training Results through NSL_KDD Dataset

During the training process, the part of the dataset that was used to train the model presented in the training process on NSL_KDD Dataset Training Results consists of 88181 records out of a total 70 percent.

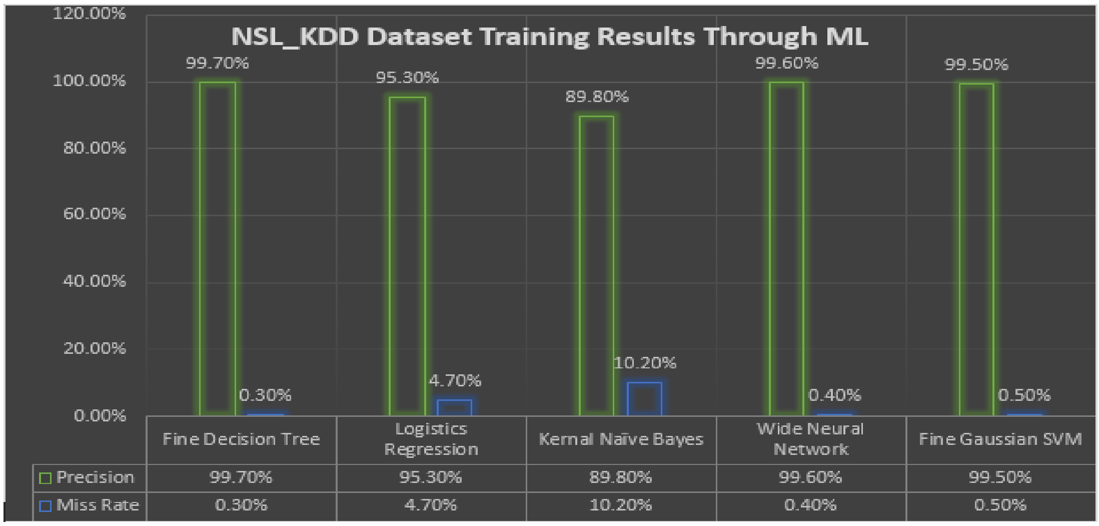


Figure 4. NSL_KDD Dataset Results training results of the Machine Learning Algorithms

In the mentioned above NSL KDD dataset training graph there was a comparative analysis of five various supervised machine learning algorithms. The resultant figure displays precision and inaccuracy of the various algorithms. The other algorithms had 99.7 percent accuracy where the Fine Decision Tree algorithms rank better in it.

4.2. Training Results through NID Dataset

The five supervised machine learning techniques have been utilized to train this model by considering a 70% Network Intrusion Detection (NID) data set of 17635 records on NID Dataset Training Results.

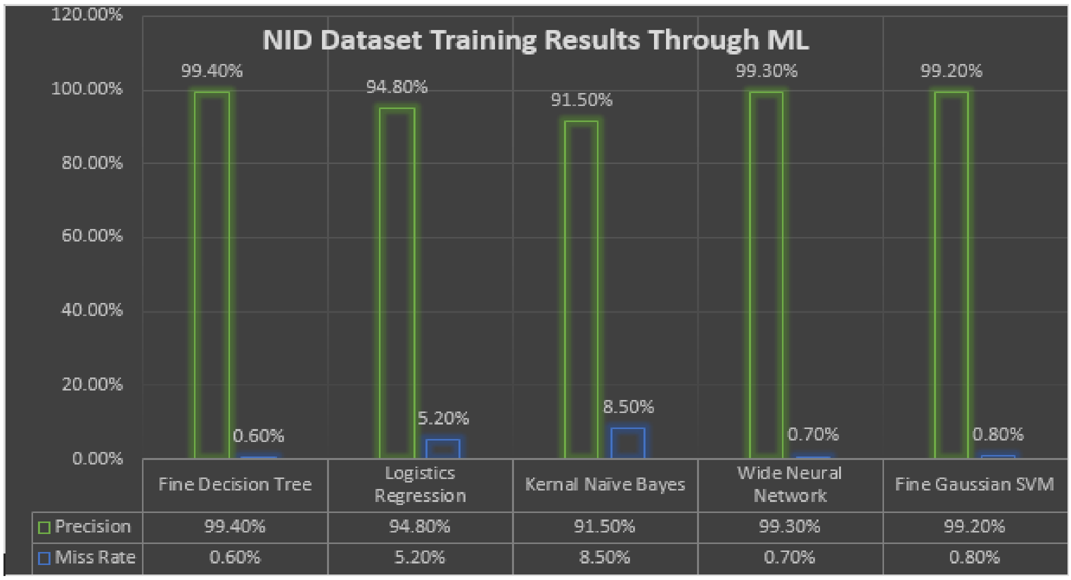


Figure 5. Training results of Machine Learning Algorithms on NID Dataset

The comparison of five different supervised machine learning algorithms has been described in the above figure in terms of NID dataset training graph. Figure the accuracy and false-hit of different algorithms is demonstrated in the figure. The best accuracy of 99.4 which is the best among all the other algorithms was accrued by the Fine Decision Tree algorithms.

4.3. Testing Results through NSL_KDD Dataset

In the testing process, 30 percent dataset, which was accessible in the form of 37792 records, was utilized to test the model with five different supervised machine learning under NSL_KDD Dataset Testing Results.

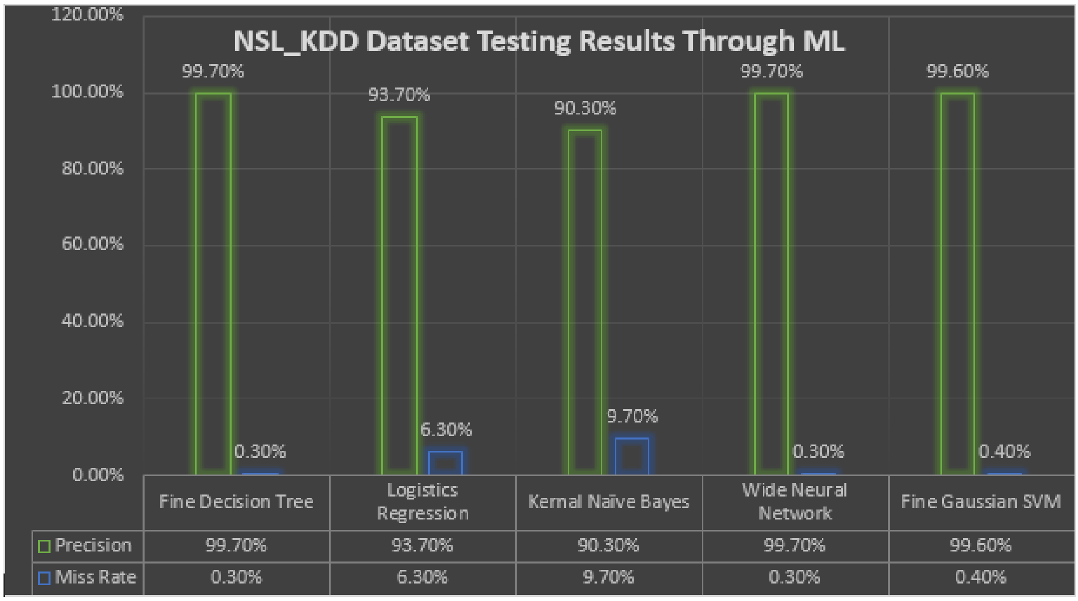


Figure 6. Test Results of Machine Learning Results on NSL_KDD Dataset

The above graph of NSL_KDD dataset training has demonstrated the comparison of five different supervised models of the machine learning. The graph indicates the accuracy and the miss rate of different algorithms. The project of the best decision tree algorithms achieved the most precise result of 99.7 percent; the accuracy in regard to accuracy of all other algorithms.

4.4. Testing Results through NID Dataset

In the phase of Testing, the model was compared with the NID dataset i.e. 7557 records in 30 percent NID was used (Test 5 supervised machine learning algorithms on NID Dataset Testing Results). Five supervised machine learning algorithms are compared in terms of training graphs of the NID dataset by using the graph that has been displayed above. The figure demonstrates precisions and miss of different algorithms. To give an example, the accuracy of Fine Decision Tree algorithms was 99.4%, which was the greatest as compared to all other algorithms.

4.5. ML Approaches Comparative Analysis on NSL_KDD and NID Datasets

Graph below indicates the performance assessment and best outcome testing with NSL_KDD and NID training sets. By way of example, the chart shows that training and testing accuracy on the NSL_KDD dataset was 99.70 and miss rate as 0.3, whereas on NID dataset accuracy was 99.40 and miss rate as 0.6.

The performance of NSL and NID dataset on in-case basis with respect to five machine-learning algorithms is indicated in the above chart. Such stat means the best delivery of the algorithms of the Decision Tree algorithms concerning the best outcome of the training and testing phase intended to examine the intrusion on the trials stage. It is therefore suggested that, early detection and blockings of attacks must be achieved through the employment of fine tree algorithms in the network industry.

4.6. Comparison of the Proposed Model with the Previous Already Published Approaches

Comparison of performance of the proposed model with the other existing approaches which various researchers used over the same data are shown in the graph below. The green line at the top indicated the accuracy of testing the fine decision tree algorithms of the proposed model that indicated that 99.40 of the algorithm accuracy. In the second line, the accuracy of the Gaussian support vector machine of the proposed model was displayed where it had 99.40 percent accuracy in NSL_KDD and NID dataset.

The accuracy of testing in terms of 98.0% shown in the graph below by [18] has used the strategy of Multilayer perceptron to analyze the NSL_KDD data. The researcher adopted a binary classification of Multilayer

Perceptron neural network with two layers of depth. The neural net determines data either as applicable to attack or not. It also explains why they use evolved 2-class approach as opposed to the correct instances classifier based on accuracy.

They employed the four different machine learning algorithms [19]. Using NSL-KDD, the researcher applied these machine-learning models in order to train and test the algorithm. It shows that the support vector computers were the outstanding among the other three algorithms, intrusion detection, random forests, decision trees and multilevel perceptrons. The presently used model of detection is a support vector machine classifier since it is predictable and also is relatively good in training data. As recommended, the testing showed 99.1 per cent precise result through a support machine.

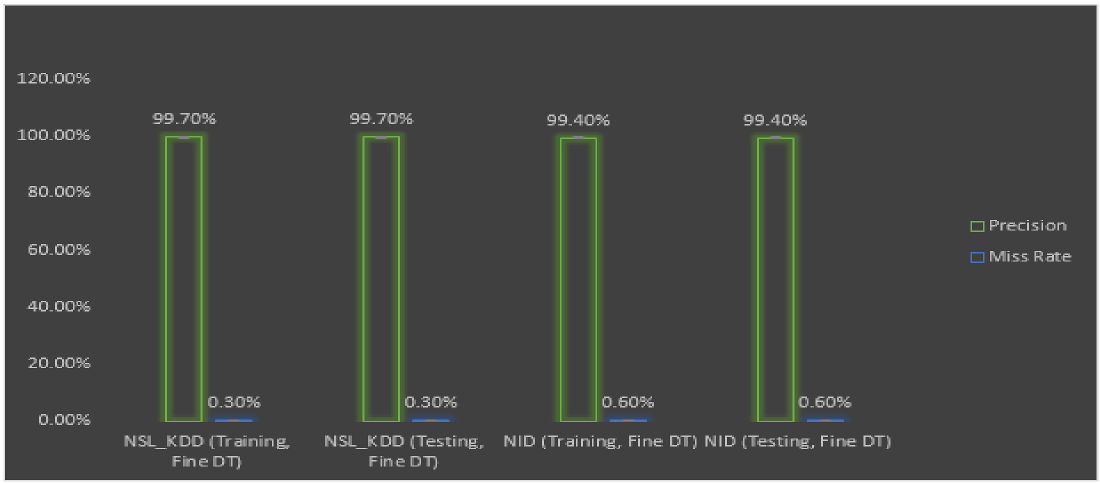
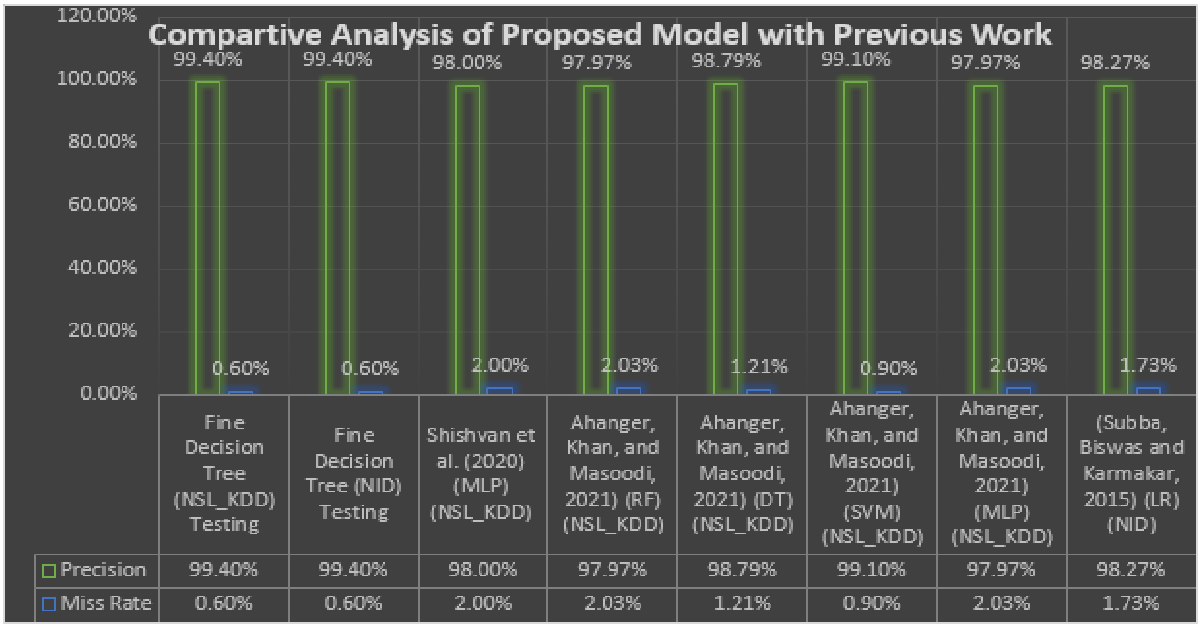


Figure 7. Comparison of Machine Learning algorithms performance on NSL_KDD and NID Data

In performance evaluation [20] demonstrated 98.27 percent testing accuracy using logistic regression algorithm against NID data set. Previous experiments have proven that the best models of IDS are those grounded on LDA and LR. LR-based systems of intrusion detection are superior because of the reduced computational effort that they impose on the models. The methodology based on Logistic Regression is precise, which is 98.27 percent.



	Fine Decision Tree (NSL_KDD) Testing	Fine Decision Tree (NID) Testing	Shishvan et al. (2020) (MLP) (NSL_KDD)	Ahanger, Khan, and Masoodi, 2021) (RF) (NSL_KDD)	Ahanger, Khan, and Masoodi, 2021) (DT) (NSL_KDD)	Ahanger, Khan, and Masoodi, 2021) (SVM) (NSL_KDD)	Ahanger, Khan, and Masoodi, 2021) (MLP) (NSL_KDD)	(Subba, Biswas and Karmakar, 2015) (LR) (NID)
🟩 Precision	99.40%	99.40%	98.00%	97.97%	98.79%	99.10%	97.97%	98.27%
🟦 Miss Rate	0.60%	0.60%	2.00%	2.03%	1.21%	0.90%	2.03%	1.73%

Figure 8. Comparison Analysis of Proposed Model with Existing ML Approaches on Network Datasets

The above graph shows the performances of the proposed model and the work that has been done in the past by some other researchers and as can be noted in the figure the proposed model had the best accuracy of all. All these algorithms would be workable in intrusion detection system, and comparing the results allows me to understand the effectiveness of such algorithms. The precise Decision Tree algorithm has a best accuracy of 99.4percent which has better potential of identifying intrusion at last stages than the other formerly published methods on the same datasets. Hence, the fine decision tree algorithms are highly advocated to be used to identify intrusion at a very early level.

5. Conclusion

Technology has led to the dependence of the world on the internet. The significance of the secure cyberinfrastructure to the society. The fast development of data and significant demand to make the networks safe against malicious attacks. Privacy between several gadgets is the hardest nut as far as now is concerned. This is the best opportunity to go down into their complex problem using machine learning. Machine learning finds application in any field in one way or another to analyzed, classify, or predict. The given model will assist in malicious traffic forecasting in the networks. The study that was proposed used the five various algorithms of supervised machine learning on the two different datasets, compared its performance to the other and recommended the most appropriate one in the network industry. Using five machine-learning algorithms, the results of the performance of NSL_KDD and NID datasets are measured. In detecting intrusion at the initial stages, there was perfection in the algorithm of Fine Decision Tree in both training and testing phases. The research has proposed that the fine decision tree got the great accuracy of 99.7 percent and 99.4 percent respectively on both datasets. Therefore this proposed model will enable the network industry to identify in much early stages malicious traffic in a network and blocking the attacks. The limitation with this study is that the results are being generated by two datasets only and few records of the dataset. A further development of this work with additional use of the various large datasets and other machine learning methods such as fusion and federated learning concept can be done in the future to enhance efficiency.

References

1. Tofan, I. and Aivaz, K.-A. (2022) "The use of computers and the internet - effects on employee productivity in Romania," *Technium Social Sciences Journal*, 32, pp. 418–429.
2. Zaripova, D. A. (2021) "Network security issues and effective protection against network attacks," *International Journal on Integrated Education*, 4(2), pp. 79–85.
3. Ball, R. (2023) "Computer viruses, computer worms, and the self-replication of programs," *Viruses in all Dimensions*, pp. 73–85.
4. Nahed, M. and Alawneh, S. (2020) "Cybersecurity in a Post-Quantum World: How quantum computing will forever change the world of Cybersecurity," *American Journal of Electrical and Computer Engineering*, 4(2), p. 81.
5. Amanowicz, M. and Jankowski, D. (2021) "Detection and classification of malicious flows in software-defined networks using data mining techniques," *Sensors*, 21(9), p. 2972.
6. Alzahrani, A.O. and Alenazi, M.J. (2021) "Designing a network intrusion detection system based on machine learning for software defined networks," *Future Internet*, 13(5), p. 111.
7. Gao, Z., 2020. Harmless Data Processing of Dead Animals in Intrusion Detection System. Revista Científica de la Facultad de Ciencias Veterinarias, 30(3), pp.1448-1459.
8. Chowdhury, M. N., Ferens, K. and Ferens, M. (2016) "Network intrusion detection using machine learning," in *Proceedings of the International Conference on Security and Management (SAM)*.
9. Kültür, E. (2022) *NETWORK INTRUSION DETECTION WITH A DEEP LEARNING APPROACH*.
10. Gabriel, I. (2020) "Artificial Intelligence, values, and alignment," *Minds and Machines*, 30(3), pp. 411–437
11. Bryndin, E. (2019) "Collaboration robots as digital doubles of person for communication in public life and space," *American Journal of Mechanical and Industrial Engineering*, 4(2), p. 35.
12. Lin, W.-C., Ke, S.-W. and Tsai, C.-F. (2015) "Cann: An intrusion detection system based on combining cluster centers and nearest neighbors," *Knowledge-Based Systems*, 78, pp. 13–21.
13. Narayan, A. and Parvat, M. (2018) "An Intrusion Detection System,(IDS) with Machine Learning (ML) Model Combining Hybrid Classifiers," *connections*, 1.
14. Ashfaq, R.A. *et al.* (2017) "Fuzziness based semi-supervised learning approach for Intrusion Detection System," *Information Sciences*, 378, pp. 484–497.
15. Mliki, H., Kaceam, A.H. and Chaari, L. (2020) "Intrusion Detection Study and enhancement using machine learning," *Lecture Notes in Computer Science*, pp. 263–278.
16. Goel, S., Guleria, K. and Panda, S.N. (2022) "Anomaly based intrusion detection model using supervised machine learning techniques," *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*.
17. Poojitha, G., Kumar, K.N. and Reddy, P.J. (2010) "Intrusion Detection Using Artificial Neural Network," *2010 Second International conference on Computing, Communication and Networking Technologies*.
18. Ahanger, A.S., Khan, S.M. and Masoodi, F. (2021) "An effective intrusion detection system using supervised machine learning techniques," *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*.
19. Shishvan, O.R., Zois, D.-S. and Soyata, T. (2019) "Incorporating artificial intelligence into Medical Cyber Physical Systems: A survey," *Connected Health in Smart Cities*, pp. 153–178.
20. Subba, B., Biswas, S. and Karmakar, S. (2015) "Intrusion detection systems using linear discriminant analysis and logistic regression," *2015 Annual IEEE India Conference (INDICON)*.